DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: F04701-03-R-0201	DUE DATE *(YYYYMMDD)*:

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*:
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.:	DATE *(YYYYMMDD)*:
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*:

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD	TBD	TBD

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		TBD

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

SMC Det 12 Space Test Engineering Contract (STEC), 2004

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)	X	
(2) Non-SCI		X
f. SPECIAL ACCESS INFORMATION	X	
g. NATO INFORMATION	X	
h. FOREIGN GOVERNMENT INFORMATION	X	
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*: Program Protection Guide	X	

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS	X	
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
l. OTHER *(Specify)*: Receive and generate sensitive-but-unclassified (SBU) data; and will have access to the government network.	X	

12. **PUBLIC RELEASE.** Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*

SMC Det 12/CCX, 3548 Aberdeen Ave SE, Kirtland AFB, NM 87117

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE.** The security classifiection guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

References to the DoD Industrial Security Manual (ISM) within this form and the contract are superseded by DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). Other security and Information Assurance Guidance for application are attached as follows:

It is the responsibility of the Prime Contractor to insure ALL of its subcontractors have a DD Form 254 on file with the Det 12 Security Officer prior to commencing any tasks.

Annex 1, Additional DD Form 254 Guidance
Annex 2, Intelligence Information
Annex 3, Special Access Information
Annex 4, Communication Security (COMSEC) Measures
Annex 5, Emissions Security (EMSEC) Measures
Annex 6, Other Security Measures
Annex 7, Marking (Furnished upon request)

Additional required distribution: in addition to block 17: SMC Det 12/PKV, VO, VOF, MST

Concur,

23 Jan 03

GARY FAIN, GS-07
SMC Det 12 Security Specialist

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. [X] Yes [ ] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)
See attached annexes

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. [X] Yes [ ] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)
See attached annexes

16. **CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.**

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
MARIA E. CHAVEZ-MANN	Contracting Officer	(505) 846-6878

d. ADDRESS *(Include Zip Code)*
SMC Det 12/PKV
3548 Aberdeen Ave SE
Kirtland AFB, NM 87117-5776

e. SIGNATURE
Maria E. Chavez-Mann

17. **REQUIRED DISTRIBUTION**

[X]	a. CONTRACTOR
[ ]	b. SUBCONTRACTOR
[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
[X]	f. OTHERS AS NECESSARY

ANNEX 1
CONTRACT NO. F04701-03-R-0201

DD FM 254 GUIDANCE

Remarks pertaining to Sections 10, 11, 12, 13, 14, and 15 are as follows:

1. SECTION 10:

1.1 Contractor personnel must possess a final U.S. Government clearance at the appropriate level and be briefed (as required) for access to the below data. A list of Contractor personnel with such accesses will be provided to the SMC Det 12 Security Office upon request. Visit requests must identify access granted and date last briefed as appropriate. The contractor shall apply all applicable markings to the material to include warning notices. All data and materials will be handled, disclosed, transmitted, reproduced and stored in accordance with the NISPOM and organizational guidance.

Item 10a: COMSEC Information - see Annex 4 for further instructions

Item 10e. Intelligence Information - see Annex 2 for further instructions

Item 10f. Special Access Information - see Annex 3 for further instructions

Item 10h. Foreign Government Information. RELEASE OF CLASSIFIED AND UNCLASSIFIED INFORMATION TO FOREIGN GOVERNMENT AND THEIR REPRESENTATIVES: Any military activity or defense contractor receiving a request from a foreign government, or a representative thereof, for classified and/or unclassified information about this program shall forward the request to SMC Det 12/VOF for the Foreign Disclosure Office (SMC Det 12/MST) approval. This does not apply to exchange or information on approved foreign military sales programs.

Item 10j: AFI 33-331 governs all For Official Use Information. Additionally, the transmittal of sensitive but unclassified or controlled unclassified across the Internet may be found in AFI 33-129.

2. SECTION 11:

2.1 Item 11c:

2.1.1 All personnel assigned to this effort that require unescorted access authority to the buildings/rooms at Kirtland AFB and Schriever must be a U.S. citizens and have a minimum of a final SECRET security clearance. A limited number of personnel must have and be able to hold a current TOP SECRET clearance.

2.1.2 The contractor will require access to classified source data up to and including TOP SECRET information in support of this work effort. Any extracts or use of such data will require the contractor to apply derivative classifications and markings consistent with the source from which the extracts were made. Refer to Annex 7, Classified Markings and Declassification Measures for further instructions.

2.1.2 See under Contract Clauses of the contract, Notification of Government Security Activity Clause, Part II. Work, to include classified automatic data processing, will be accomplished at prime contractor facilities, Kirtland AFB, and Schriever AFB. When processing classified information on government furnished automated information systems (AIS) the contractor shall comply with all applicable DOD, Air Force, HQ AFSPC, HQ AFMC, and local Security Measures. It is the contractor's responsibility to understand these publications (e.g., directives, instructions, manuals, plans) and obtain either a hard copy or soft copy from the office providing support to, the Procurement Contracting Officer, Security Office, and/or Information Assurance Office.

2.2 **Item 11l:** Sensitive-but-Unclassified (SBU) automatic data processing will occur at the prime contractor facilities, Kirtland AFB and Schriever AFB. The contractor will also be granted access to networks at these locations or interface between these sites via the Internet. When processing SBU information on either government-furnished or contractor systems, ADPE prior approval must be granted by the SMC Det 12 Information Assurance Office. Information of an SBU nature will not be placed on the Internet without approved and tested access and security controls. This includes information that falls under the definition of Personal or Privacy Act, For Official Use Only, Scientific, Technical or Research and Development.

3. SECTION 12:

There will be no voluntary public release of information. Requests for public release of information concerning this contract shall be submitted through SMC Det 12/VOF to SMC Det 12/CCX as appropriate, 45 days in advance of scheduled release date. Answers to queries may be made only with the express approval of the SMC Det 12/CCX , 3548 Aberdeen Ave SE, Kirtland AFB NM 87117-5778. No other dissemination of information is authorized. This prohibition extends to all publications of an informational nature both internal and external, and to all conversations except those required for conduct of official business.

4. SECTION 13:

4.1 Executive Order 12958, Classified National Security Information, contains new classification, declassification, and marking requirements which **are not** the same as those of the NISPOM. The Marking Guide at Annex 7 is provided on specific instructions while the NISPOM is being revised to incorporate these changes. Unless approved by the Contracting Officer the Contractor **does not** have to remark existing classified documents to comply with the new requirements.

4.2 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls must be public access information. The following types of unclassified information **shall not** be placed on the Internet without approved and tested access and security controls: (a) For Official Use Only; (b) Personal or Privacy Act; (c) Scientific, Technical or Research and Development; and, (d) Unclassified information that requires special handling. Refer to AFI 33-331 to address For Official Use Only Application.

4.3 Refer to Annex 6, Other Security and Protection Measures, with regard to Security Classification Guidance and Program Protection information.

5. SECTION 14: Additional security requirements, in addition to the NISPOM and associated annex(es), are established. Refer to the appropriate annex to the DD Fm 254 for these requirements and guidelines.

6. SECTION 15: The Defense Security Service is relieved of inspection responsibilities.

ANNEX 2
CONTRACT NO. F04701-03-R-0201

SENSITIVE COMPARTMENTED INFORMATION

1. GENERAL

a. Physical Security

This contract requires access to Sensitive Compartmented Information (SCI). The assistant Chief of Staff for Intelligence, USAF, has exclusive security responsibility for all SCI classified material released to or developed under this contract. This SCI information must be maintained in a Sensitive Compartmented Information Facility (SCIF). DCID 6/4, 6/9, DoD 5105.21-M-l and AFM 14-304 serves as the necessary guidance for physical, personnel, and information security measures and are part of the security specification for this contract. Contractor compliance with these directives is mandatory unless specifically waived. Inquiries pertaining to classification guidance for SCI will be directed to SMC/INS through the Contract Monitor. The contractor is required to comply with the physical security standards as defined in DCID 6/9, DOD 5105.21-M-l and AFM 14-304. SCI material released to the contractor under this contract shall be stored and worked on only within the proposed facility and upon receipt of an approved physical security accreditation by SSO DIA/DAC. AFSPC sponsored SCIF shall not be co-utilized with other government agencies unless covered by an approved Co-Utilization Agreement (CUA). The User Agency SSO is SMC/INS, Los Angeles AFB, CA. Work performed under this contract shall not be accomplished in a SCIF accredited by another Government Organization unless there is an approved CUA between that organization and SMC/INS. Applicable Program Security Classification guidance will be identified in block 13 of this DD Form 254.

b. Personnel Security

The contractor shall nominate a CSSO and Alternate to SMC/INS. No contractor will be granted access to SCI information/material under this contract unless they are filling a SMC/IN SCI billet assigned under this contract. The names of contractor personnel requiring accessing to SCI will be submitted to SMC/INS through the Contract Monitor. Upon receipt of a completed background investigation the CSSO will submit a request for SCI eligibility to SMC/INS in accordance with AFM 14-304. Contract employees sponsored by other than Agencies/Organization shall be certified to SMC/INS through the Servicing SSO for access to a SMC Programs. The contractor shall establish and maintain a current billet roster indicating accesses of SCI personnel on this contract. A copy of this list shall be provided to SMC/INS through the Contract Monitor annually, or as changes occur. The contractor shall also advise SMC/INS through the Contract Monitor immediately upon the reassignment of personnel to duties not associated with this contract, to include termination.

c. **Document Control**

SCI furnished in support of this contract remains the property of the SMC Program Office releasing it. The contractor shall maintain an active accountability of all SCI material received, produced, maintained, and disposed of that is in their custody. Upon completion or cancellation of this contract, SCI data will be returned to the custody of the government (Program Office) unless a follow-on contract specifies that material will be transferred to that contract. Inventories of SCI material will be conducted in accordance with DOD 5105.21-M-1 and AFM 14-304. Any supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency Special Security Office (SMC/INS)

d. **Release of Information**

SCI will be released to contractors only when originator approval has been obtained. The contractor may release such material to any contractor employee assigned to a billet and indoctrinated for Program SCI access under this contract and only when a need-to-know exists. The contractor may release such material to any Special Security Office personnel assigned to HQ SMC, HQ Air Force Space Command (AFSPC), HQ USAF, or DIA upon demand. The contractor shall not release this material to other contractor, subcontractor, or Federal Government agency employees unless the Program Office, Contract Monitor, or SMC/INS has granted prior written approval. An access certification to an SMC contractor occupied SCIF does not constitute approval to release SMC contractual material to other contractor, subcontractor, or federal government employees: SMC/INS or Contract Monitor approval is required. SCI will not be released to non-U.S. citizens. SMC/INS approval of an SMC contractor visit certification or permanent certification to another facility will constitute approval to discuss contractual information/material at the facility to be visited.

e. **Reproduction of SCI Information**

The contractor may reproduce any SCI related to this contract at the discretion of the Contract Special Security Officer (CSSO), as long as the copies are controlled in the same way as the originals and they remain in the SCIF. No copies of SCI documents will be transferred to other contractors.

f. **Sub-Contracting**

A CSSO shall coordinate with the Contract Monitor and obtain the concurrence of SMC/INS prior to subcontracting any portion of SCI efforts involved in this contract.

g. **Public Release**

The contractor shall not make references to SCI even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.

2. **BLOCK 10k: Other: Automated Information Systems**

Comply with DOD 5105.21-M1 Chapters 7 and 8, DIAM 50-4, AFM 14-304 Chapters 7 & 8. The Contractor CSSO shall submit a Systems Security Concept of Operations and an AIS Security Operations Procedure/Standard Practice Procedure.

3. **BLOCK 11i TEMPEST Requirements**

TEMPEST security measures must be considered if electronic processing of SCI is involved in accordance with DOD 5105.21-M1 Chapter 7 and Appendix J; AFM 14-304, Chapter 7

4. **BLOCK 11k Defense Courier Service**

This contract requires the use of the Defense Courier Service (DCS). The CSSO will prepare and submit DCS Form 10 in original triplicate to SSO SMC/INS for validation prior to their submittal to the appropriate DCS station (reference to Block 11k).

5. **BLOCK 14 Additional Security Requirements**

The following Directives, Manuals, Instructions, Handbook, or Pamphlet are incorporated into this contract as they pertain to the access, handling, control, dissemination, processing of Sensitive Compartmented Information:

DCID 6/4
DCID 6/9
DOD 5105.21-M1
DIAM 50-4
AFM 14-304

6. **BLOCK 15 Inspections**

Defense Security Service is relived of inspection responsibilities pertaining to Sensitive Compartmented Information associated with this contract. The following activity is designated as inspection authority and the User Agency SSO for SCI requirements in accordance with DOD 5105.21-M-l, and AFM 14-304.

SMC/INS (SMC SSO)
2420 Vela Way, Suite 1467
Los Angeles AFB
El Segundo, CA 90245-4659

The User Agency Special Security Officer (SSO) is:

SMC/INS

(310) 363-0175

The Alternate Special Security Officer (ASSO) is:

SMC/INS
(310) 363-1585

ANNEX 3
CONTRACT NO. F04701-03-R-0201

SPECIAL ACCESS INFORMATION

1. Special Access Information:

a. The contractor shall establish a point of contact for Special Access Required (SAR) security matters. This individual will have responsibility for all SAR security matters within the contractor's facility, in accordance with the appropriate SAR Security Guide.

b. The contractor shall establish and maintain an access list of those employees approved by the contract monitor for SAR portions of the contract. A copy of this list will be furnished to SMC Det 12 Security Office.

c. The contractor will advise SMC Det 12 Security Office and immediately upon reassignment of SAR accessed personnel to other duties not associated with this contract.

ANNEX 4
CONTRACT NO. F04701-03-R-0201

COMMUNICATIONS SECURITY (COMSEC) MEASURES

1.0 **GENERAL.** The contractor shall, in addition to the requirements set forth in the DoD National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-R), NSAM 90-1, Oct 2001, comply with the written instructions of the installation Commander regarding communications security matters.

2.0 **PURPOSE**. Provides for additional security measures required by the Government to be taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information.

3.0 **REFERENCE**. Item 11h of the DD Fm 254

4.0 COMSEC AND/OR CRYPTOGRAPHIC ACCESS

4.1 COMSEC material/information may not be released to DoD contractors without Air Force Crytological Support Center (AFCSC) approval. Contractor must forward request for COMSEC material/information to the COMSEC Officer through the program office. The contractor is governed by NSAM 90-1, Oct 2001 in the control and protection of COMSEC material/information. Access to COMSEC material/information is restricted to U.S. citizens holding final U.S. government clearances and is not releasable to personnel holding only a reciprocal clearance.

4.2 The Air Force program/project manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis.

4.3 The COMSEC/CRYPTO briefing applies only to the use and control of crypto equipment and specialized COMSEC publications. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment will not be retained in a contractor facility.

5.0 INTERNET POLICY AND ENCRYPTION

5.1 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls, must be public access information.

ANNEX 5
CONTRACT NO. F04701-03-R-0201

EMISSIONS SECURITY (EMSEC) MEASURES

1.0 PURPOSE. Provides for additional security measures required by the Government to be taken to deny information which might be derived from the interception of compromising emanations from electronic equipment.

2.0 REFERENCES. Items 11C and 11I of the DD Fm 254

3.0 TEMPEST REQUIREMENTS:

3.1 The contractor shall ensure that compromising emanations conditions related to this contract are minimized. The contractor shall provide TEMPEST Countermeasures Assessment (TCA) information to the Contracting Officer and he/she will forward it to the Government EMSEC focal point (Det/MST). This information will be used by the Government EMSEC focal point to assess the contractor's facility. A contractor's standard security plan is unacceptable as a "stand-alone" facility information document. EMSEC requirements also apply to subcontractors; however, they should not be imposed without prior approval of the Government Contracting Office. When imposed, TCA information on the subcontractor must be submitted through the prime contractor to the Government Contracting Office. The TCA will be performed by the Government TEMPEST authority using current Air Force EMSEC directives.

3.2 The contractor should not expend any resource other than providing the TCA information until the TEMPEST assessment is completed and direction is provided through the contracting officer. TEMPEST is applied on case-by-case basis and further information may be required to complete the TCA; should this be the case, the contractor will provide this information to the Contracting Officer when requested. During the facility assessment period, contractors should reply to questions with specific and timely answers.

3.3 Equipment used by the contractor to process SECRET information must at a minimum meet the TEMPEST Red/Black separation requirement listed on the attached sheet. Based on the results of the TCA additional requirements may be imposed.

3.4 The contractor must submit to the Program Management Office (Det 12/VOF) an Equipment Change Notification (ECN) to advise the PMO of any proposed change or relocation of equipment used to process SECRET (or higher) information. The ECN must be submitted at least 30 days before the change or relocation occurs.

3.5 The contractor must submit to the PMO a new TCA at least 30 days before processing SECRET or higher information in a different facility than that specified in the original TCA.

3.6 Classified processing shall not commence until the TCA has been evaluated and approved by the Government TEMPEST authority, and the Automated Data Products (ADP) procedures have been approved by the Cognizant Security Office. The contractor will then be notified by the contracting officer that classified processing can begin.

4.0 TEMPEST COUNTERMEASURES ASSESSMENT INFORMATION FORMAT

(See above paragraph)

4.1 System Description Data:

4.1.1 System/Facility: Provide full name and address of company submitting request and RFP/contract number and duration. Provide names and addresses of additional facilities and subcontractors, if any, that will process SECRET or higher information in support of this contract. A separate TCA must be performed by the Government TEMPEST authority for each facility that will process SECRET or higher information. Also provide a brief title identifying the overall system or facility (i.e., test launch facility, command post word processing system, plans and programs interactive graphics, system, etc.).

4.1.2 Location: Identify the address (including city, state, facility, building and room number) where the system and facility are located. Facility diagrams (outer perimeter) and floor plans for each floor and room that will be processing classified information must be submitted.

4.1.3 Equipment: List the manufacturer and exact model number, nomenclature (terminal, disk drive, video systems, etc.) and quantity of each piece of equipment involved in classified processing.

4.2 Responsible Personnel. Provide Security Officer/Manager and System Custodian point of contact name, title, office symbol and phone number for each facility. Include the Company Appointed TEMPEST Authority (CATA) if there is one.

4.3 Operational Risk: Estimate the percent of total material processed for each level of classification. Estimate the volume on a per day basis by bytes, lines, pages or hours for each classification. If the same equipment will be used for classified processing in support of other projects, list classification(s) and percentage(s) of use by other programs.

4.3.1 Physical Security: Provide information on security procedures for control of personnel gaining access to the buildings and rooms (i.e., key card access, security desk, cipher lock access, etc.) where classified processing will be done.

4.3.2 Give brief description of building (brick, wooden, windows, number of floors, loading docks, etc.).

4.4 Remarks. Provide any amplifying information that could assist in determining the hazard and risk situation for the facility in question.

5.0 TEMPEST SEPARATION REQUIREMENTS

5.1 Countermeasures Application. These paragraphs discuss how to apply the countermeasures and under what conditions they would not be required.

5.1.1 Keep RED and BLACK signal lines separated. Keeping RED signal lines about six inches away from BLACK signal lines will reduce coupling to a level low enough to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

5.1.2 Keep RED signal lines separated from BLACK Power lines. Keeping RED signal lines about six inches away from BLACK power lines will reduce coupling to a low enough level to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

5.1.3 Keep RED processors separated from BLACK telephones and telephone lines. Keep non-TEMPEST-approved printers at least six feet away from telephones. Do not use the telephone while printing classified information. Keep all non-TEMPEST-approved equipment at least three feet away from the telephone lines; two inches if the telephone lines are shielded.

6.0 TEMPEST SEPARATION MATRIX

RED/BLACK	CRYPTO EQUIPMENT	UNSHIELDED SIGNAL AND TELEPHONE LINES	SHIELDED TELEPHONE LINES	POWER LINES
Crypto Equipment	0000	3ft	2in	2in
Unshielded Signal Lines	6in	6in	3in	6in
Shielded Signal Lines	2in	2in	2in	2in
TEMPEST-Approved Equipment	2in	6in	2in	NONE
Non-TEMPEST-Approved Equipment	3ft	3ft	2in	NONE

ANNEX 6
CONTRACT NO. F04701-03-R-0201

OTHER SECURITY AND PROTECTION MEASURES

1.0 SECURITY CLASSIFICATION GUIDES

Security Classification Guides (SCG) to include any changes or revisions will be made available to the contractor in performance of contractual tasks as required.

2.0 PROTECT GUIDES

The National Security Policy and DoD Space Policy and supplements require RDT&E entities develop protect guides for major systems and support capabilities. This is an effort to reduce the number of SCGs and focus information classification at the system level. Applicable SCG content however will be considered when developing protect guides for SMC Det 12. Protect guides are also developed for modernization and development, test and operations purposes. Contractor agencies will be required to participate (i.e., provide existing documents and attend meetings) in applicable protect guides development. Protect guides to include any changes or revisions will be made available to the contractor in the performance of contractual tasks as required.

3.0 PROGRAM PROTECTION PLAN

A Program Protection Plan (PPP) is required in accordance with AFI 31-7, Acquisition Security. The Air Force will integrate security needs and requirements into a PPP beginning in Phase 0 of an acquisition program and maintain this plan throughout the system's life. Contractor agencies will be required to participate (i.e., provide existing documents and attend meetings) in applicable PPP development. The PPP to include any changes or revisions will be made available to the contractor in the performance of contractual tasks as required.

4.0 ORIGINAL CLASSIFICATION AUTHORITY (OCA) AND DECLASSIFICATION AND DOWNGRADING AUTHORITY (DDA)

4.1 Delegation and Authorization. The Secretary of the Air Force is responsible to make appointments and delegations, in accordance with Executive Order 12958, of those Air Force positions authorized to originally classify and declassify or downgrade classified information and their level of authority. For example, only an OCA can classify information at the level authorized, and only a DDA can authorize declassification or downgrading of that information. The contractor's classification of information is derivative to the original guidance, and actions to declassify or downgrade this information should be in accordance with DDA guidance. This guidance is generally provided in the form of an SCG but may also be provided by other written medium.

4.2 Classification Challenges. Requests to challenge information classification, or to have information declassified or downgraded outside of its specified time, should be submitted through the SMC Det 12 Security Office for OCA and DDA action. Pending an OCA or DDA reply the classified information will be handled at its current level of classification.

5. INTERNATIONAL PROGRAMS SECURITY

The contractor shall ensure full compliance with DOD (e.g., DODD 5230.11) , Air Force (e.g., AFI 16-201, AFI 61-204), supporting major commands supplements, and, local guidance on International Program security requirements. Applicable guidance will be timely implemented and enforced to effect proper access and protection of affected governmental functions under this contract. This includes import/export, documentation and technology marking (e.g., warning, distribution statements, FOIA requirements), discussions and meetings with foreign entities to include those via networks and other related international program security requirements. Any classified or controlled unclassified military information (CUMI), also known as controlled export technical data, and, technology to be released must have approval by the Foreign Disclosure Office prior to release. The contractor shall ensure full compliance with the International Traffic in Arms Regulations, and must be able to obtain and maintain the necessary license and agreements (e.g., technical assistance agreement) required in support of this contract.

6. NATIONAL SECURITY INFORMATION MARKING

Executive Order 12958 requires that classified national security information be marked to place recipients on alert about its sensitivity. The pamphlet that provides a general guide on these marking requirements is available to the contractor upon request through the SMC Det 12 Security Office.

ANNEX 7

CONTRACT NO. F04701-03-R-0201

MARKING

Furnished upon request